Sulla risoluzione degli indirizzi IP Parte II – Domain Name System

Stefano Bonacina (*), Francesca Giuratrabocchetti (**), Davide Stefanoni (***)

(*) *Dottorato di Ricerca in Bioingegneria – XVI ciclo – Politecnico di Milano*
(**) *CILEA, Segrate*
(***) *già Politecnico di Milano e Medical Informatics Training Program of the National Library of Medicine (NLM) at the National Institute of Health (NIH), Bethesda, MD, USA*

Abstract
Prosegue anche in questo numero la pubblicazione di una monografia a puntate sul riconoscimento degli indirizzi IP. Il lavoro è originato dalla attività di dottorato di Stefano Bonacina, dottorando in Bioingegneria del Politecnico di Milano. Il documento originale è stato curato e rivisto nel suo complesso dagli specialisti di reti del CILEA, anche per tenere conto delle attuali evoluzioni delle soluzioni software.
Questa seconda parte descrive il Domain Name System, il servizio software che si occupa di tradurre gli indirizzi numerici, adatti ai computers, in nomi a dominio, più adatti agli umani.

Keywords: Telematica, TCP/IP, DNS, Reti.

I componenti fondamentali del Domain Name System

Il DNS ha tre componenti principali [1]:

1. Il DOMAIN NAME SPACE (SPAZIO dei NOMI di DOMINIO) ed i RESOURCE RECORDS (RECORD di RISORSA), i quali caratterizzano uno spazio di nomi strutturato ad albero ed i dati associati ai nomi. Concettualmente, ogni nodo e foglia dell'albero dello spazio dei nomi di dominio stabilisce un insieme di informazioni, e per estrarre specifici tipi di informazioni da un particolare insieme vengono eseguite operazioni di interrogazione. Una interrogazione, *query* è il termine inglese, stabilisce il nome di dominio di interesse e descrive il tipo di informazione di risorsa che è desiderato. Per esempio, usa alcuni dei suoi nomi di dominio per identificare host; le query per le risorse indirizzo restituiscono gli indirizzi degli host di Internet.
2. I NAME SERVERS sono programmi server che tengono informazioni circa la struttura ad albero del dominio, e le informazioni di insieme. Un *name server* può depositare la struttura o le informazioni di insieme circa qualsiasi parte dell'albero di dominio, ma, in generale, un particolare *name server* contiene informazioni complete di un sottoinsieme dello spazio dei domini, e puntatori ad altri *name server* che possono essere usati per ottenere informazioni da qualsiasi parte dell'albero dei domini. I *name server* conoscono le parti dell'albero dei domini per le quali essi dispongono di informazioni complete; un *name server* è detto essere una AUTHORITY per queste parti dello spazio dei nomi. Le informazioni autoritarie sono organizzate in unità chiamate ZONE, e queste zone possono essere automaticamente distribuite ai *name server*, i quali forniscono un servizio ridondante per i dati in una zona.
3. I RESOLVER sono programmi che estraggono informazioni dai *name server* in risposta alle richieste dei client. I resolver devono essere in grado di accedere ad almeno un *name server* ed usare le informazioni di quel *name server* per rispondere direttamente a query, o per rilanciare la query usando riferimenti ad altri *name server*. Un resolver è tipicamente una routine di sistema che è direttamente

accessibile ai programmi utente; per tale ragione nessun protocollo è necessario tra il resolver ed il programma utente.

Sintassi dei nomi di dominio

Il DNS usa un sistema gerarchico di assegnazione dei nomi conosciuto come *nomi a dominio*. Un nome di dominio consiste in una sequenza di sotto-nomi separati dal carattere punto. Nel nome di dominio ogni sezione è comunemente chiamata *etichetta* o semplicemente *dominio* (Figura 1).

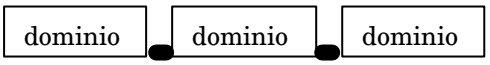

Figura 1 - Struttura di un nome di dominio.

Ogni dominio è di competenza di una specifica autorità secondo un preciso schema gerarchico. Si definisce Fully Qualified Domain Name (FQDN) il nome di dominio a più basso livello, cioè quel nome che include tutti i domini di livello superiore al suo. Un FQDN è anche detto nome di dominio completo o semplicemente *host name*. Se si pensa al DNS come ad un albero, il FQDN di un certo nodo è costituito dal nome del nodo seguito da quello di tutti gli altri nodi tra esso e la radice dell'albero. In sostanza si tratta di risalire l'albero fino alla radice leggendo via via tutti i nodi che si incontrano. La Figura 2 mostra una piccola parte della gerarchia dei nomi di dominio della rete Internet.

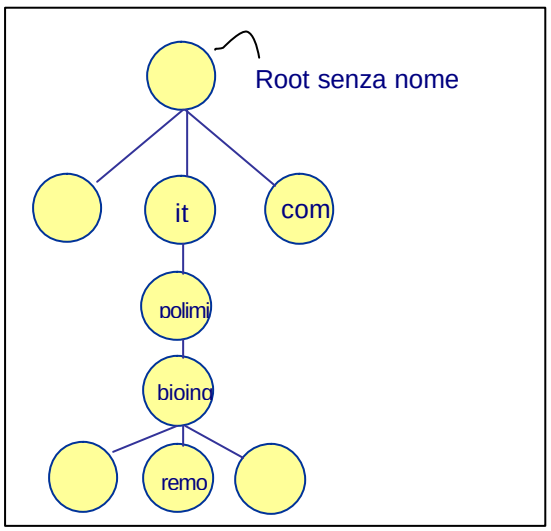

Figura 2 - Struttura di un nome di dominio.

Nell'esempio di Figura 2 il nome di dominio completo è remo.bioing.polimi.it e indica un computer del Dipartimento di Bioingegneria del Politecnico di Milano. Il dominio di terzo livello è bioing.polimi.it e indica la rete del Dipartimento di Bioingegneria del Politecnico di Milano. Il dominio di secondo livello è polimi.it e indica la rete del Politecnico di Milano. Il dominio di più alto livello, comunemente detto Top Level Domain,TLD, è infine .it e indica il paese in cui il dominio è stato registrato. Come mostra l'esempio, i nomi di dominio vengono scritti a partire dal più specifico (più lontano dalla radice) verso il meno specifico (più vicino alla radice). Dato che un nome di dominio completo finisce con l'etichetta radice, e che questa è sempre rappresentata da una stringa nulla, un nome completo finisce sempre con un punto. Se non viene specificato il punto, quello che si ottiene è un nome incompleto. Di solito i nomi incompleti vengono completati automaticamente dal software, provando con il dominio locale e con alcuni domini predefiniti, tra cui il punto '.' indicante la radice. Quindi se viene omesso il punto finale quando si digita un nome di dominio, questo viene facilmente riconosciuto come un nome da risolvere rispetto al dominio radice.

Il dominio radice, o dominio di root, che si trova a capo dell'albero contiene un elenco di tutti i server DNS dei domini di primo livello. Sparsi per Internet esistono una decina di DNS radice, ma sono usati solo per creare ridondanza e contengono tutti le stesse informazioni. I domini di primo livello, Top Level Domain in inglese, avente per acronimo TLD, sono indicati in Tabella 1. Sono detti domini generici, gTLD, cioè generic Top Level Domain.

Sigla del gTLD	Descrizione
ARPA	Vecchio stile Arpanet
COM	Organizzazioni Commerciali USA
EDU	Università USA
GOV	Organizzazioni Governative USA
INT	Organizzazione Internazionale
MIL	Enti Militari USA
NATO	Ambito Nato
NET	Network
ORG	Organizzazioni No-Profit

Tabella 1 - Sigle dei Top Level Domain e loro significato.

Il giorno 16 novembre 2000, la ICANN annunciò che sette nuovi generici Top Level Domain sarebbero stati selezionati per cominciarne l'uso nel 2001 [2]. I nuovi gTLD, conosciuti anche come "estensioni Web", sono stati selezionati in base a parecchi fattori, ma con lo scopo principale di continuare la rapida crescita di Internet. Nella Tabella 2 sono riportati i nuovi TLD e la loro descrizione.

Sigla del gTLD	Descrizione
BIZ	Per uso commerciale di aziende e individui.
INFO	Per uso senza restrizioni, generale.
NAME	Per uso limitato alla registrazione di individui.
PRO	Per uso limitato a professionisti (commercialisti, avvocati, medici) ed associazioni di professionisti.
AERO	Per uso riservato alle compagnie aeree.
COOP	Per uso riservato a cooperative aziendali.
MUSEUM	Per uso riservato ai musei.

Tabella 2 - Sigle dei sette nuovi Top Level Domain e loro significato.

Esistono domini di primo livello di sole due lettere (stabilite dallo standard ISO 3166) per i domini geografici, come ad esempio **.it** per l'Italia, **.fr** per la Francia, **.de** per la Germania, **.uk** per il Regno Unito e così via: prendono il nome di ccTLD (Country Code TLD). Al di sotto dei domini di alcuni paesi esiste una gerarchia che rispecchia quella dei domini di primo livello. Ad esempio i nomi delle organizzazioni commerciali di Regno Unito (**.uk**) e Giappone (**.jp**) finiscono rispettivamente in **.co.uk** e **.co.jp**, mentre l'equivalente dei **.edu** sono **.ac.uk** e **.ac.jp** (dove ac è l'abbreviazione di "academic"). Anche per gli Stati Uniti è stato previsto il codice **.us** anche se in realtà le organizzazioni statunitensi non ne fanno uso e adottano prevalentemente i TLD **.com**, **.edu**, e **.gov**. Il dominio di primo livello **.us**, indicante gli Stati Uniti d'America, si usa in combinazione con il codice di ogni singolo stato componente (ad esempio **.md.us** indica lo stato del Maryland).

La conversione dei nomi di dominio in indirizzi numerici IP

Il Domain Name System, DNS, è una base di dati distribuita che permette il controllo locale dei nomi di dominio su segmenti della rete Internet. Questo significa che non esiste un unico computer che conosce l'indirizzo IP di tutte le macchine collegate ad Internet, a differenza di quanto avveniva usando il file HOSTS. Le informazioni sono invece distribuite su migliaia di calcolatori, ognuno dei quali è responsabile di una certa porzione del nome, detta dominio o zona di autorità. I programmi che gestiscono questi segmenti di rete sono denominati Name Server Primari o semplicemente DNS. Per ogni zona viene allestito almeno un altro server DNS, detto Secondario, per ragioni di *fault tolerance:* esso contiene una copia delle informazioni del primario. Ad intervalli prefissati (la cui lunghezza è modificabile dall'amministratore del servizio) il DNS secondario interroga il primario per controllare se ci sono variazioni nella tabella dei domini indirizzati. In caso affermativo questa viene copiata nel secondario [3].
Sinteticamente è possibile definire un *name server*, o *server* DNS, come un *host* in grado di fornire la traduzione di un nome di dominio in un indirizzo IP e viceversa. Il computer che fornisce questo servizio può rispondere direttamente alle richieste riferite ai nomi di dominio di competenza della sua zona, e per gli altri, deve interpellare altri *name server* competenti. I server sono organizzati secondo una struttura gerarchica ad albero che presenta forti somiglianze con la struttura del file system del sistema operativo UNIX.

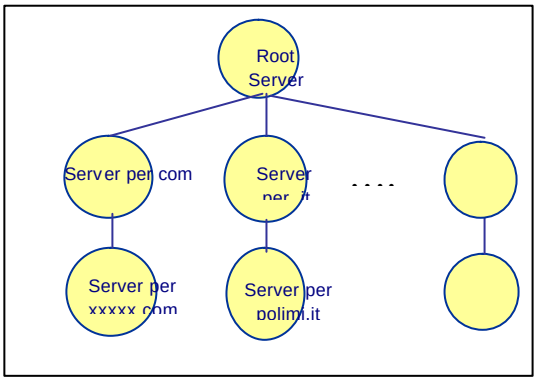

Figura 3 - La sistemazione concettuale dei server di nomi di dominio in un albero che corrisponde alla gerarchia dei nomi.

Si tratta di un albero al cui capo troviamo il dominio radice (di solito denotato con un punto '.') e dove ogni nodo dell'albero corrisponde ad un dominio, o equivalentemente, al server DNS che lo gestisce, Figura 3. Le foglie dell'albero

sono i nomi dei calcolatori. Un server DNS che copre un dominio di primo livello conosce gli indirizzi di tutti i DNS di secondo livello sottostanti ad esso. A sua volta un server DNS di secondo livello conosce gli indirizzi di tutti i DNS di terzo livello e così via. Quindi un DNS .it conosce tutti i domini del tipo *qualche-cosa.it* ed i rispettivi indirizzi numerici. Un DNS di secondo livello di una certa organizzazione conosce, a sua volta, tutte le macchine il cui nome Internet finisca con *nome-organizzazione.it*.

Se i server DNS lavorassero come suggerisce il modello sin qui presentato, le relazioni tra la gerarchia dei nomi e l'albero dei server sarebbe alquanto semplice. In realtà l'albero dei server DNS ha un minor numero di livelli poiché un singolo server può fisicamente contenere le informazioni di una larga parte della gerarchia dei nomi. In particolare le organizzazioni spesso raccolgono le informazioni da tutti i propri sotto-domini in un singolo server [3]. La Figura 4 mostra una rappresentazione maggiormente aderente alla realtà rispetto allo schema precedente.

Poiché l'albero ha una struttura piatta e larga, cioè pochi livelli ma molto popolati, un minor numero di server devono essere contattati per risolvere un nome di dominio. Il programma server dispone di un database DNS che contiene record standardizzati chiamati *Resource Record* (RR, Record delle Risorse). I Resource Record collegano i nomi agli indirizzi host e specificano altri parametri operativi del DNS.

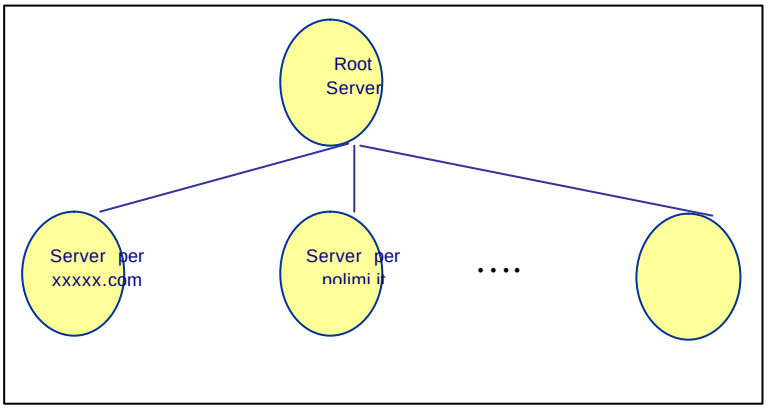

Figura 4 - La reale organizzazione dei server dei server di nomi di dominio in un albero che corrisponde alla gerarchia dei nomi.

Struttura del database Domain Name System

Il database DNS comprende quattro tipi di file, di cui due contenenti gli RR:

- il *file di boot* contiene le informazioni principali di configurazione sul server DNS, inclusa l'ubicazione degli altri file di configurazione. Il file di boot è unico.
- il *file di cache* contiene una "cache di avvio" che elenca i server dei nomi principali da interrogare quando il server locale non è in grado di soddisfare una richiesta basandosi sulla sua cache o sul database interno. Anche il file di cache è unico.
- I *file di zona* contengono gli RR e altre informazioni di definizione di un dominio. Ciascun dominio ha un file di zona separato, quindi se si serve più di un dominio ci saranno diversi file di zona.
- I *file di zona speciali* vengono forniti dal software DNS e solitamente sono statici (cioè questi file vengono usati così come vengono forniti dal rivenditore). Un file di zona speciale piuttosto diffuso è il file di zona db.0.0.127, necessario per alcune implementazioni TCP/IP.

Un database DNS può essere suddiviso in più *zone*. Una zona è una parte di database DNS contenente i record di risorse con i nomi dei proprietari appartenenti ad aree adiacenti dello spazio dei nomi DNS. I file di zona vengono gestiti sui server DNS. Un server DNS può

essere configurato in modo da contenere una o più zone o da non contenerne alcuna.

Il file di boot

È il file di configurazione principale utilizzato dal name server al momento della sua attivazione. La struttura di un file di boot è la seguente [1]:

```
; Boot file for name server
directory      /etc/named

; type domain source-file
cache  .      named.cache

------ BOOT.ZONES ------
; type      domain                      source-file
primary  nomedominio.esempio.it      named.hosts
primary  0.0.127.IN-ADDR.ARPA        named.local
primary  123.123.123.IN-ADDR.ARPA    named.rev
```

La riga di comando che inizia con directory definisce il path, ovvero il percorso, per gli altri file di configurazione del name server . La riga che comincia con cache indica il file *root.cache* che contiene tutti i DNS server del mondo che si trovano alla root o comunque al livello superiore della gerarchia dei DNS mondiali. Viene rappresentato con un punto ('.') . Questo file varia rapidamente e deve essere aggiornato. E' possibile prelevare gli aggiornamenti di questo file direttamente da Internet all'indirizzo:

ftp.rs.internic.net / domain / named.root .

Questo file è indispensabile se i calcolatori di una Intranet devono poter accedere ad Internet, in caso contrario è bene eliminare questa opzione oppure renderla una nota di commento facendola precedere dal carattere punto e virgola:

;cache . named.cache

In questo modo si nega l'accesso esterno ai calcolatori della rete Intranet, i quali non potranno richiedere nomi su Internet ad alcun DNS.
I file *named.host*, *named.local*, *named.rev* corrispondono ai rispettivi file di zona per i domini indicati. In particolare è importante notare che il dominio 0.0.127.IN-ADDR.ARPA si riferisce alla configurazione per la rete 127.0.0.0, cioè quella del localhost. Mentre il domino 123.123.123.IN-ADDR.ARPA si presenta come indirizzo ribaltato ed è relativo al file *named.rev* contenente il "reversal" dei vari IP della rete. In questo file viene stabilita la configurazione per la rete locale 123.123.123.

Il file di zona

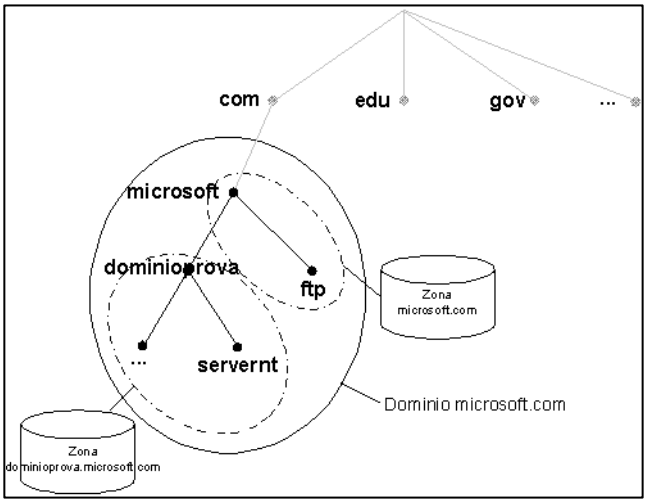

Figura 5 – Esempio di suddivisione di un dominio in zone

Ciascuna zona è legata a un particolare nome di dominio che costituisce il *dominio principale* della
Zona, Figura 5. Una zona contiene informazioni relative a tutti i nomi che terminano con il nome del dominio principale della stessa. Un server DNS viene considerato autoritativo per un nome se "carica", contiene, la zona contenente tale nome. Il primo record di un file di zona è un RR Start Of Authority (SOA, Origine di autorità). Il record SOA identifica un server DNS primario per la zona come migliore origine di informazioni per i dati all'interno della zona e come entità di elaborazione degli aggiornamenti per la zona.
I nomi all'interno di una zona possono inoltre essere delegati ad altre zone. La delega è un processo di assegnazione di responsabilità per un'area di uno spazio dei nomi DNS a un'entità a parte. Questa entità separata può essere un'organizzazione, un reparto o un gruppo di lavoro diverso all'interno di un'azienda. In termini tecnici, la delega implica l'assegnazione di autorità su aree dello spazio dei nomi DNS ad altre zone. Tale delega viene rappresentata dal record NS che specifica la zona delegata e il nome DNS del server considerato autorevole per questa zona. La delega tra più zone era compresa nei progetti originali del DNS.

Le ragioni principali che determinano la delega di uno spazio dei nomi DNS possono essere:

- Necessità di delegare la gestione di un dominio DNS a una quantità di organizzazioni o reparti all'interno di un'azienda
- Necessità di distribuire il compito di gestire un unico database DNS di grosse dimensioni tra più server dei nomi per migliorare le prestazioni di risoluzione dei nomi e per creare un ambiente DNS a tolleranza di errore.

I record NS semplificano la delega mediante l'identificazione dei server DNS per ciascuna zona. Appaiono in tutte le zone di ricerca diretta e inversa. Quando un server DNS deve effettuare una ricerca su zone diverse da quella di cui è autorevole tale server farà riferimento ai record NS relativi ai server DNS nella zona di destinazione.

Ogni dominio servito ha un file di zona separato, solitamente denominato per convenzione con il prefisso db, seguito dal nome del dominio completo o parziale. Il vero nome del file di zona è irrilevante in quanto il file di boot collega il nome del dominio ad un particolare file indipendentemente dal suo nome. Tuttavia, se si usano nomi correlati al dominio si semplifica la manutenzione, soprattutto se si servono domini multipli. Un file di zona contiene gli RR che definiscono le singole conversioni nome-indirizzo per quel dominio. Il formato di base di un RR è:

nome TTL classe tipo dati

Lo scopo e il significato dei singoli campi sono:

- *Nome*. Questo campo deve iniziare nella colonna uno e identifica l'host o il dominio descritto dal record.
- *TTL*. Il campo TTL (Time To Live, tempo di vita) specifica il numero di secondi durante i quali un altro server dei nomi terrà registrato il record nella cache prima di cancellarlo. Nella maggior parte dei file di zona questo valore non viene codificato in quanto si usa un valore predefinito fornito nell'RR SOA (Start of Authority).
- *Classe*. Si codifica sempre questo campo come IN per rappresentare una rete di classe Internet. Dato che il DNS è stato utilizzato prima che Internet diventasse di fatto la rete standard, la sintassi RR supporta altri tipi di classi a cui nessuno è più interessato. Solo la classe IN è valida per l'uso in Internet.
- *Tipo.* Un file di zona contiene tipi RR diversi per vari scopi. Ne esistono una ventina ma comunemente vengono usati solo sei tipi di RR che verranno descritti successivamente. Gli altri tipi non sono molto usati e non necessario conoscerli per utilizzare i file di zona DNS Internet.
- *Dati.* Il contenuto del campo dati dipende dal tipo di record. Nella maggior parte degli RR il campo dati si compone di uno o due valori. In un particolare RR del file di zona (l'RR SOA), tuttavia, il campo dati è molto lungo e solitamente si estende su più righe.

Tipi di Resource Record

Ogni file di zona ha determinati Resource Record di intestazione indispensabili, seguiti da uno o più RR di dettaglio.

Record Start of Authority (SOA)

Il record Start of Authority (SOA), il primo record di intestazione, definisce alcuni parametri del dominio per il quale questo file di zona è l'autorità suprema. Un record SOA indica che questo file è *la* fonte definitiva delle informazioni per il dominio, quindi può esistere un solo SOA al mondo per un dato dominio.
Esempio:

```
@       IN SOA      nshost.nomedominio.esempio.it indirizzoemail.esempio.it
                                (1995061403     ; Serial
                                    300         ; Refresh - 5 Minutes
                                    60          ; Retry - 1 minute
                                    1209600     ; Expire - 2 Weeks
                                    43200)      ; Minimum - 12 Hours
```

Un record SOA è strutturato nel modo seguente:

```
nome IN SOA dns-primario contatto-amministrativo (
        numero seriale
        limite di tempo per aggiornamento
        limite di tempo per nuovi tentativi
        limite di tempo per la scadenza
        limite di tempo minimo)
```

Il nome di dominio codificato nel campo *nome* identifica il dominio al quale si applica questo SOA ed è spesso indicato dal carattere "@" che si riferisce al dominio associato a questo file nel file di boot. Il campo dati dell'RR SOA ha più parti. In primo luogo, il campo contiene due nomi: il server DNS primario per il dominio e l'indirizzo di posta elettronica del contatto amministrativo del dominio; gli indirizzi di posta elettronica nel DNS utilizzano un punto invece di una "at" (@). Questi sono campi di sola documentazione (si forniscono questi campi per far sì che gli altri utenti di Internet possano determinare il nome del server e la persona responsabile dell'amministrazione del dominio). Segue una serie di cinque valori che controllano il modo in cui il file di zona interagisce con il resto della rete Internet. Il record SOA è l'unico RR che può essere posto su più righe.

Il valore del *numero seriale* serve per il controllo della versione e deve essere incrementato ogni volta che si aggiornano i record del file di zona. I server secondari (di backup) utilizzano il numero seriale per determinare quando la loro copia dei dati deve essere aggiornata. Può essere lungo fino a 10 cifre.

Il *limite di tempo per aggiornamento* specifica la frequenza con cui un server secondario (di backup) deve controllare per vedere se il file primario è stato cambiato o meno. Solitamente questo valore è compreso tra una e sei ore (da 3.600 a 21.600 secondi).

Il *limite di tempo per nuovi tentativi* determina quanto tempo attende un server secondario prima di tentare di contattare il server primario nel caso in cui il server primario diventi inaccessibile. Un buon limite di tempo per i nuovi tentativi è da 20 a 60 minuti (da 1.200 a 3.600 secondi).

Il *limite di tempo per la scadenza* determina per quanto tempo i server secondari continuano a servire i dati del dominio quando il server primario non è contattabile. La maggior parte degli amministratori DNS imposta questo valore su una settimana (604.800 secondi) o più.

Il *limite di tempo minimo* è il valore TTL di default indicante quanto a lungo un RR rimane valido nella cache di un server DNS remoto. Per comodità solitamente non si codifica un valore TTL in ogni RR: è molto più semplice codificarlo una volta in questo punto del file e farlo diventare il default per tutti i record RR del file. Questo valore determina quanto si deve aspettare dopo aver apportato un cambiamento prima di essere certi che tutti, su Internet, ottengano i nuovi valori.

Record NS

Il successivo RR di intestazione, il record NS, Name Server (= Server dei nomi), definisce i server dei nomi autoritari per la zona. Si definisce un record NS per il server primario e uno per ciascun server secondario. Il formato è il seguente:

dominio *IN NS* *nome-server-dns*

Il nome del dominio nel campo del nome identifica il dominio per il quale si applica questo RR NS. Il campo dati è il nome completamente qualificato del server DNS e quindi deve terminare con un punto. Il nome del server DNS dovrebbe essere un nome canonico, cioè un nome per il quale esiste un record di tipo **A** corrispondente.

Esempio: nomedominio.esempio.it. IN NS
nshost.nomedominio.esempio.it.
IN NS offnet.host.nomedominio.esempio.it

Record Address, A

Il record A, ossia di indirizzo, costituisce il nucleo del file di zona. Questi record forniscono la proiezione nome host - indirizzo IP che è la parte centrale del DNS. Un file di zona contiene

un record A per ciascun host che si desidera identificare in modo unico nella rete. Il nome host nel campo nome si converte nell'indirizzo IP posto nel campo dati del record A. Il formato è il seguente:

nomehost IN A indirizzoip

Esempio: nomehost.nomedominio.esempio.it.
IN A 111.122.133.1

Record MX

I record MX (Mail eXchange = Scambio posta) definiscono gli host che forniscono il servizio di scambio postale per un dominio. Solitamente, quando un utente indirizza della posta Internet ad un altro utente presso un dominio, l'utente mittente non sa quale host gestisce la posta per il dominio; il record MX consente al server postale del mittente di determinare quale host contattare per la posta in entrata. Inoltre, il record MX è in grado di fornire una lista di host per gestire la posta in modo che quando il server postale primario diventa inoperabile possa intervenire un server postale di backup. Il DNS consente di avere server postali ridondanti per facilitare la ricezione della posta. Il formato del record MX è il seguente:

dominio IN MX preferenza nomehost

Il campo *preferenza* permette di specificare l'host a cui si preferisce venga inviata la posta: i server postali di backup hanno valori di preferenza numericamente superiori all'host preferito. Infatti zero è il valore che indica la massima preferenza, mentre 65535 è quello che indica la preferenza minima.

Record Canonical Name, CNAME

Un host può essere noto con più di un nome; si usano i record CNAME per definire nomi aggiuntivi, chiamati soprannomi o alias, per un particolare host. I record CNAME associano un alias al nome reale di un host. Si usano gli alias quando un host fornisce più di un servizio e tale servizio ha un nome convenzionale su Internet. Ad esempio, i server Web sono ben noti su Internet con l'alias "www", i server FTP sono noti con l'alias "ftp". Se si deve spostare un servizio su un altro host, è sufficiente cambiare il CNAME per fare riferimento al nuovo host, eliminando quindi la necessità di informare gli utenti della modifica. Il formato del record CNAME è il seguente:

alias IN CNAME nomehost

Occorre sottolineare che gli alias sono stati creati per l'uso da parte dei soli utenti Internet e non come un'abbreviazione da usare nei file DNS. Ogni volta che è necessario specificare un nome host nel campo dati di un RR, si deve usare il nome reale e non un alias.

Record PTR

Il record PTR definisce le conversioni indirizzo numerico-nome, note come "ricerche DNS inverse". Il formato del record PTR è il seguente:

indirizzoip IN PTR nomehost

Il record PTR consente agli altri siti Internet di determinare il nome dell'host e il nome del dominio partendo da un indirizzo IP. Questo è spesso necessario quando, ad esempio, il browser contatta un server remoto e il server remoto registra il contatto per nome. Il server riceve solamente l'indirizzo IP e non il nome, quindi è necessario convertire l'indirizzo IP in un nome in modo da poter registrare il contatto. Gli indirizzi sono da intendersi assoluti perché indicati con un punto finale.
Esempio:

```
1    IN PTR  nomehost1.nomedominio.esempio.it.
2    IN PTR  nomehost2.nomedominio.esempio.it.
```

Il numero che appare all'inizio indica un nome di dominio abbreviato che rappresenta un collegamento con i record A. Il dominio di origine di questo file, si vedano gli esempi mostrati in precedenza, è **133.122.111.in-addr.arpa.**
I nomi di dominio completi sono:

```
1.133.122.111.in-addr.arpa        IN PTR
  nomehost1.nomedominio.esempio.it.
2.133.122.111.in-addr.arpa        IN PTR
  nomehost2.nomedominio.esempio.it.
```

Cioè l'indirizzo IP di:
nomehost1.nomedominio.esempio.it
è 111.122.133.1 e, in modo del tutto analogo, quello di:
nomehost2.nomedominio.esempio.it
è 111.122..133.2.
Tramite i record **A** possono essere abbinati più nomi di dominio allo stesso indirizzo numerico, ma con i record **PTR** si può abbinare un indirizzo numerico a un solo nome di dominio.

Bibliografia

[1] Mockapetris PV. RFC1034. *Domain names – concepts and facilities,* novembre1987.
Disponibile all'indirizzo URL:
http://isc.faqs.org/rfcs/rfc1034.html
Data ultimo accesso: 5 febbraio 2003

[2] ICANN. *Top-level domains*.
Disponibile all'indirizzo URL:
http://www.icann.org/tlds/.
Data dell'ultimo accesso: 5 febbraio 2003

[3] Fuller V, Li T, Yu J, Varadhan K. RFC1519. *Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy,* settembre 1993.
Disponibile all'indirizzo URL:
http://isc.faqs.org/rfcs/rfc1519.html
Data ultimo accesso: 5 febbraio 2003.